情報ネットワーク学　期末レポート

2017/07/27

37-176843 中川大海

テーマ：AI によるサイバー攻撃対策

1. テーマの概要

近年相次いでいる情報漏えい事件やサイバー攻撃は、日本のみならず世界中で問題となっており、時には国家レベルの危機にさえなっている。これらの脅威に備えるために次世代ファイアウォール、IDS/IPS、WAF、Web フィルタリング、アンチウィルスなどさまざまな対策が打たれているが、どれも事後的・対症的なアプローチであり、次々に現れるウィルスなどによる攻撃を完全に防御することは困難である。そこで近年注目されているのが、情報セキュリティへの AI の活用である。

2. テーマの具体的内容

一口に AI の活用といってもそのアプローチは様々だが、最も一般的なのは機械学習によるパターン検出エンジンとしての適用である。膨大な数のシステムログやイベントを統合的に収集・管理し、横断的に分析することで脅威をいち早く検知・対処することを目的としている。

具体的な事例としては、MIT が開発した、85%のサイバー攻撃を自動検出し、偽陽性も従来の 1/5 程度に抑えることを可能にした AI プラットフォーム「Squared」や、ソフトバンクが出資した米国ベンチャーのサイバーリーズン社によるサイバー攻撃対策、NTT コミュニケーションズが開発した、不審な通信を自動検知して遮断する AI などがある。

このように、各社でサイバー攻撃のパターン認識技術の研究が進んでいるが、今後さらに重要になってくるのが、こうした断片的な技術を集積して自律的に情報管理の行えるネットワークシステムの開発だと言われている。例えば、マルウェア感染対策についても、単にマルウェアのパターン認識を行うだけでなく、ユーザーの普段の Web アクセスの様子から、マルウェアに

感染しやすい行動をしているユーザーを監視して、感染を起こす前に対策を講じるといったアプローチなどがある。

3. テーマに対する自分の意見

AI によるサイバー攻撃対策のトレンドは今後ますます盛んになってくると思うが、偽陽性・偽陰性率と、安全性・信頼性などのトレードオフをどうバランスをとるかは、ユーザーへの浸透が重要なこの分野においては常に課題となる観点だと考えられる。

また、IoT 化が進み、これまでネットワークに組み込まれていなかったような、人間生活のリアルな部分がネットワーク化されていく時代においては、個別デバイスや個別目的の認識エンジンだけでは対応に限界が出て来ると考えられ、より統合的なセキュリティ AI システムの開発は重要だと感じた。

ただ、サイバー攻撃の対策側での AI 活用が進む一方で、攻撃側にも AI 活用の利は存在すると考えられるため、攻撃を完全に遮断できるようなシステムの構築にはまだまだ時間がかかると考えられる。攻撃側の AI 活用に遅れを取らず、より高い防御性を獲得するために AI 活用の研究は重要だが、技術の限界を補うためにも、情報を扱う人間側のセキュリティ意識が再度重要になると考えられ、そうした教育や啓蒙を推進する技術以外の方面でのアプローチも検討が必要だと感じた。

具体的な AI 技術としては、従来の識別的なアプローチだけでなく、サイバー攻撃側と検知側のモデルを学習させる GAN などの生成的アプローチや、エージェントにサイバー攻撃検知・対策などを学習させる強化学習的なアプローチの活用も有効なのではないかと感じた。近年深層学習技術の活用によってこれらの分野も発展しており、これらの技術を活用することでより柔軟なサイバーセキュリティ AI を開発できると考えられる。

参考

http://it-trend.jp/cyber_attack/article/use_of_ai
http://jp.techcrunch.com/2017/05/13/20170512las-vegas-taps-ai-for-cybersecurity-help/
https://japan.zdnet.com/article/35081389/
http://itpro.nikkeibp.co.jp/atclact/active/17/021600024/030700017/